

REMARKS

Claims 1, 2, 4, 6-18, and 20-35 are currently pending in the subject application and are presently under consideration. Claims 1, 14, 20, 28 and 33-35 have been amended as shown on pp. 2-9 of the Reply. Claims 11-13 have been canceled.

Applicants' representative thanks the Examiner for the courtesies extended during the teleconference of September 22, 2008.

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 20-27, and 33-35 Under 35 U.S.C. §101

Claims 20-27, and 33-35 stand rejected under 35 U.S.C. §101 because the claimed invention is directed to non-statutory subject matter. Applicants' representative respectively disagrees.

Further, independent claim 20 has been amended herein to clearly illustrate that elements within such claims are components associated with a computer processor. In particular, claim 20 as amended is directed towards a system comprising ***a processor for executing the following components:*** a code generator, a code hiding module, a decoder, a tracing component and a pseudo random number generator, wherein the components perform a function (*e.g.*, generate a first code, create a second code, determine the first code from the new code, determine whether a user accessing the first code is a valid user and generate pseudo random numbers). (Support for these amendments can be found on pg. 7, lines 1-14 and pg. 24, lines 21-28). Accordingly, this claim includes functional descriptive material within a processor, thereby rendering it structurally and functionally interrelated to the processor and is therefore directed to statutory subject matter. Claim 33-35 have been amended to overcome any deficiencies related to this rejection. Accordingly, this rejection should be withdrawn with respect to claims 20-27 and 33-35.

II. Rejection of Claims 1-2, 4, 6, 11-12, 15-16, 20, 28, 30-31, and 33-35 Under 35 U.S.C. §102(e)

Claims 1-2, 4, 6, 11-12, 15-16, 20, 28, 30-31, and 33-35 stand rejected under 35 U.S.C. §102(e) as being anticipated by Moskowitz (US 2008/0046742). It is respectfully requested that this rejection should be withdrawn for at least the following reasons. Moskowitz does not teach or suggest each and every element as set forth in the subject claims.

The claimed subject matter relates to a first code that is designed within the noise model, and performs various algebraic transformations on such first code to create a second code. Upon transforming the first code into the second code, the second code will appear to be random to a computationally bounded adversary. Therefore an adversarial attack on the second code will essentially be a noise attack on the first code, as the attack will be randomly distributed across the first code. Randomly distributing the attack across the first code allows the code to act as it was designed – with respect to random noise. Thus the first code can be associated with error correction/detection properties when random noise is applied to the first code.

Independent claim 1 recites a system that facilitates efficient code construction, comprising: *a component that receives a first code designed in a noise model,...; and a transformation component that transforms the first code to a new code that has essentially same length parameters as the first code but is hidden to a computationally bounded adversary, ..., wherein the new code acts as a protective wrapping of the first code, such that an attack on the new code by the computationally bounded adversary would appear as a noise attack on the first code, as the attack would be randomly distributed across the first code and not concentrated on a particular location within the first code, this allows the first code to act as it was designed to and utilize the algorithms to correct the noise errors with a high success rate; ...; and a tracing component that determines whether a user accessing the first code is a valid user via a unique watermark associated with a particular user and embedded in the first code, wherein if the watermark does not correlate to an authorized user, access is denied; and a pseudo random number generator, the pseudo random number generator generates two pseudo random numbers a and b , each n number of bits, based upon a position within the sequence of one of the messages, and further generates a random permutation σ that permutes the n bits.*

Moskowitz does not expressly or inherently disclose the aforementioned novel aspects of applicants' claimed subject matter as recited in the subject claims.

Moskowitz discloses a system for encoding digital watermark information in a signal. The system includes a window identifier for identifying a sample window in the signal; an interval calculator for determining a quantization interval of the sample window; and a sampler for normalizing the sample window to provide normalized samples. Further, the system includes a processor for identifying an area of the digital signal that will be affected by the digital filter and an encoder for encoding the at least one digital watermark in the digital signal. The encoder encodes the digital watermark so as to avoid the area of the digital signal that will be affected by the digital filter. (See pg. 2, paragraphs [0010]-[0011]).

In contrast, applicants' claimed subject matter discloses a system that includes a code generator that generates a code designed in a noise model. The code is then relayed to a code hiding module that facilitates randomizing the code, thereby hiding the code from potential and/or actual adversaries.

More particularly, the code generator includes an encoding function f that encodes a plurality of messages into the code. Thus, the code is generated based upon a sequence of t messages $m_1, m_2, m_3, \dots, m_i, m_{i+1}, \dots, m_t$, where each message m is k bits in length. The code generator therefore generates the code *via* sequentially encoding each message (e.g., $f(m_i)$). The code hiding module receives the code in a sequence of $f(m_1), f(m_2), \dots, f(m_i), \dots, f(m_t)$, and *via* utilizing a pseudo random number generator generates two pseudo random numbers of n bits, a and b for each encoded message, where $a \neq 0$. These pseudo random numbers are generated based upon a position within the sequence of each encoded message m . The code-hiding module also utilizes the pseudo random generator to generate a random permutation σ to permute n bits. The code-hiding module can then send $a \times \sigma(f(m_i)) + b$ (e.g., code 2), where \times is a bitwise multiplication operator, over a channel and to a receiver that includes a decoder. While resident within the channel, a noise vector can be added to code 2. For example, a vector v (adversarial in nature) of Hamming weight w can be added to code 2 by the channel. Therefore the decoder receives $a \times \sigma(f(m_i)) + b + v$. (See pg. 12, lines 13-27).

Moskowitz does not disclose a system that utilizes a pseudo random number generator that generates two pseudo random numbers based upon a position within the sequence of one of

the messages, and further generates a random permutation. Moskowitz simply provides for correction of random bit errors and burst errors, such that highly redundant error codes and interleaving might create a buffer against burst errors introduced into digital watermarks through randomization attacks. Moskowitz does not disclose a first code generated based at least in part on a sequence of messages.

Accordingly, Moskowitz is silent with regard to a system that facilitates efficient code construction, comprising: ..., *a pseudo random number generator, the pseudo random number generator generates two pseudo random numbers a and b , each n number of bits, based upon a position within the sequence of one of the messages, and further generates a random permutation σ that permutes the n bits.*

Furthermore, independent claim 20 recites a system that hides a codeword from a computationally bounded adversary, comprising: *a code generator that generates a first code designed in a noise model and based at least in part upon a sequence of messages that are desirably relayed to a receiver, ... , wherein the second code acts as a protective wrapping of the first code, such that an attack on the second code by the computationally bounded adversary would appear as a noise attack on the first code, as the attack would be randomly distributed across the first code and not concentrated on a particular location within the first code, this allows the first code to act as it was designed to and utilize the algorithms to correct the noise errors with a high success rate; a tracing component that determines whether a user accessing the first code is a valid user via a unique watermark associated with a particular user and embedded in the first code, wherein if the watermark does not correlate to an authorized user, access is denied; and a pseudo random number generator, the pseudo random number generator generates two pseudo random numbers a and b , each n number of bits, based upon a position within the sequence of one of the messages, and further generates a random permutation σ that permutes the n bits.*

As stated *supra*, Moskowitz does not disclose a system that utilizes a pseudo random number generator that generates two pseudo random numbers based upon a position within the sequence of one of the messages, and further generates a random permutation. Moskowitz simply provides for correction of random bit errors and burst errors, such that highly redundant error codes and interleaving might create a buffer against burst errors introduced into digital

watermarks through randomization attacks. Moskowitz does not disclose a first code generated based at least in part on a sequence of messages.

Further, independent claim 28 recites a method for hiding a data package from a computationally bounded adversary, comprising:....; *algebraically transforming the encoded message into a first code, the first code rendered random to an unauthorized user, and the first code comprising algorithms utilized to correct noise errors with high probability; transforming the first code to a second code that has essentially same length parameters as the first code but is hidden to a computationally bounded adversary, wherein the second code acts as a protective wrapping of the first code, such that an attack on the second code by the computationally bounded adversary would appear as a noise attack on the first code, as the attack would be randomly distributed across the first code and not concentrated on a particular location within the first code; utilizing the algorithms of the first code to correct the noise errors with a high success rate; and determining whether a user accessing the first code is a valid user via a unique watermark associated with a particular user and embedded in the first code, wherein if the watermark does not correlate to an authorized user, access is denied; and **generating two pseudo random numbers a and b , each n number of bits, based upon a position within the sequence of one of the messages, and further generating a random permutation σ that permutes the n bits.***

As stated *supra*, Moskowitz does not disclose a system that utilizes a pseudo random number generator that generates two pseudo random numbers based upon a position within the sequence of one of the messages, and further generates a random permutation. Moskowitz simply provides for correction of random bit errors and burst errors, such that highly redundant error codes and interleaving might create a buffer against burst errors introduced into digital watermarks through randomization attacks.

Further, independent claim 33 recites a system that facilitates efficient code construction, comprising: ... *means for generating two pseudo random numbers a and b , each n number of bits, based upon a position within the sequence of one of the messages, and further means for generating a random permutation σ that permutes the n bits.*

Moskowitz does not disclose a system that utilizes a pseudo random number generator that generates two pseudo random numbers based upon a position within the sequence of one of

the messages, and further generates a random permutation. Moskowitz simply provides for correction of random bit errors and burst errors, such that highly redundant error codes and interleaving might create a buffer against burst errors introduced into digital watermarks through randomization attacks.

Further, independent claim 34 recites a computer readable medium having computer executable instructions stored thereon to transfer a first code into a second code, ... *a pseudo random number generator, the pseudo random number generator generates two pseudo random numbers a and b, each n number of bits, based upon a position within a sequence of one of the messages, and further generates a random permutation σ that permutes the n bits.*

Moskowitz does not disclose a system that utilizes a pseudo random number generator that generates two pseudo random numbers based upon a position within the sequence of one of the messages. Moskowitz simply provides for correction of random bit errors and burst errors, such that highly redundant error codes and interleaving might create a buffer against burst errors introduced into digital watermarks through randomization attacks.

Furthermore, independent claim 35 recites a computer readable medium having a data structure stored thereon that receives a first code that is designed in a noise model and transforms the first code into a second code, ... *a pseudo random number generator, the pseudo random number generator generates two pseudo random numbers a and b, each n number of bits, based upon a position within a sequence of one of the messages, and further generates a random permutation σ that permutes the n bits.*

Moskowitz does not disclose a system that utilizes a pseudo random number generator that generates two pseudo random numbers based upon a position within the sequence of one of the messages. Moskowitz simply provides for correction of random bit errors and burst errors, such that highly redundant error codes and interleaving might create a buffer against burst errors introduced into digital watermarks through randomization attacks.

In view of the aforementioned deficiencies of Moskowitz, it is respectfully submitted that this rejection be withdrawn with respect to independent claims 1, 20, 28 and 33-35 (and claims 2, 4, 6, 11, 12, 15-16 and 30-31 which respectively depend there from).

III. Rejection of Claims 7-8, 25, and 29 Under 35 U.S.C. §103(a)

Claims 7-8, 25, and 29 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Moskowitz (US 2008/0046742) in view of Cox (US 6,275,965). It is respectfully submitted that this rejection should be withdrawn for the following reasons. Moskowitz and Cox *et al.*, individually or in combination, do not teach or suggest each and every element set forth in the subject claims. In particular, Cox *et al.* does not make up for aforementioned deficiencies of Moskowitz with respect to independent claims 1, 20 and 28 (which claims 7-8, 25 and 29 depend respectively there from). Thus, the claimed subject matter as recited in claims 7-8, 25 and 29 is not obvious over the combination of Moskowitz and Cox *et al.* Therefore, it is respectfully submitted that this rejection be withdrawn.

IV. Rejection of Claims 9 and 10 Under 35 U.S.C. §103(a)

Claims 9 and 10 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Moskowitz (US 2008/0046742) in view of Guruswami (Foundations of Computer Science, 2001, Proceedings, 42nd IEEE Symposium, Pages 658-667, ISBN: 0-7695-1116-3). It is respectfully submitted that this rejection should be withdrawn for the following reasons. Moskowitz and Guruswami, individually or in combination, do not teach or suggest each and every element set forth in the subject claims. In particular, Guruswami does not make up for aforementioned deficiencies of Moskowitz with respect to independent claim 1 (which claims 9 and 10 depend there from). Thus, the claimed subject matter as recited in claims 9 and 10 is not obvious over the combination of Moskowitz and Guruswami. Therefore, it is respectfully submitted that this rejection be withdrawn.

V. Rejection of Claims 13-14, 17-18, and 32 Under 35 U.S.C. §103(a)

Claims 13-14, 17-18, and 32 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Moskowitz (US 2008/0046742) in view of Venkatesan *et al.* (US 6,829,710). It is respectfully submitted that this rejection should be withdrawn for the following reasons. Moskowitz and Venkatesan *et al.*, individually or in combination, do not teach or suggest each and every element set forth in the subject claims. In particular, Venkatesan *et al.* does not make up for aforementioned deficiencies of Moskowitz with respect to independent claims 1 and 28 (which claims 13-14, 17-18 and 32 depend respectively there from). Specifically, Venkatesan

et al. merely discloses providing a water mark that is associated with a pre-defined function of the code. In contrast, applicants' claimed subject matter discloses a unique watermark embedded within the first code and *associated with a particular user*. If the watermark does not correlate to an authorized user of the file, then access is denied. Thus, the claimed subject matter as recited in claims 13-14, 17-18 and 32 is not obvious over the combination of Moskowitz and Venkatesan *et al.* Therefore, it is respectfully submitted that this rejection be withdrawn.

VI. Rejection of Claims 21-23 Under 35 U.S.C. §103(a)

Claims 21-23 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Moskowitz (US 2008/0046742) in view of Bohnke (US 6,557,139). It is respectfully submitted that this rejection should be withdrawn for the following reasons. Moskowitz and Bohnke *et al.*, individually or in combination, do not teach or suggest each and every element set forth in the subject claims. In particular, Bohnke *et al.* does not make up for aforementioned deficiencies of Moskowitz with respect to independent claim 20 (which claims 21-23 depend there from). Thus, the claimed subject matter as recited in claims 21-23 is not obvious over the combination of Moskowitz and Bohnke *et al.* Therefore, it is respectfully submitted that this rejection be withdrawn.

VII. Rejection of Claim 24 Under 35 U.S.C. §103(a)

Claim 24 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Moskowitz (US 2008/0046742) in view of Bohnke (US 6,557,139) in further view of Guruswami (Foundations of Computer Science, 2001, Proceedings, 42nd IEEE Symposium, Pages 658-667, ISBN: 0-7695-1116-3). It is respectfully submitted that this rejection should be withdrawn for the following reasons. Moskowitz, Bohnke *et al.*, and Guruswami, individually or in combination, do not teach or suggest each and every element set forth in the subject claims. In particular, Guruswami does not make up for aforementioned deficiencies of Moskowitz and Bohnke *et al.* with respect to independent claim 20 (which claim 24 depends respectively there from). Thus, the claimed subject matter as recited in claim 24 is not obvious over the combination of Moskowitz, Bohnke *et al.* and Guruswami. Therefore, it is respectfully submitted that this rejection be withdrawn.

VIII. Rejection of Claims 26 and 27 Under 35 U.S.C. §103(a)

Claims 26 and 27 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Moskowitz (US 2008/0046742) in view of Tian *et al.* (US 6,714,683). It is respectfully submitted that this rejection should be withdrawn for the following reasons. Moskowitz and Tian *et al.*, individually or in combination, do not teach or suggest each and every element set forth in the subject claims. In particular, Tian *et al.* does not make up for aforementioned deficiencies of Moskowitz with respect to independent claim 20 (which claims 26-27 depend there from). Thus, the claimed subject matter as recited in claims 26-27 is not obvious over the combination of Moskowitz and Tian *et al.* Therefore, it is respectfully submitted that this rejection be withdrawn.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP588US].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,

AMIN, TUROC & CALVIN, LLP

/Marisa J. Zink/

Marisa J. Zink

Reg. No. 48,064

AMIN, TUROC & CALVIN, LLP
24TH Floor, National City Center
1900 E. 9TH Street
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731